

# On generalizations of Fermat curves over finite fields and their automorphisms

**Nazar Arakelian**

CMCC, Universidade Federal do ABC, Santo André, Brazil

**Pietro Speziali**

Univesità Degli Studi della Basilicata, Potenza, Italy

August 16, 2016

## Abstract

Let  $\mathcal{X}$  be an irreducible algebraic curve defined over a finite field  $\mathbb{F}_q$  of characteristic  $p > 2$ . Assume that the  $\mathbb{F}_q$ -automorphism group of  $\mathcal{X}$  admits as an automorphism group the direct product of two cyclic groups  $C_m$  and  $C_n$  of orders  $m$  and  $n$  prime to  $p$  such that both quotient curves  $\mathcal{X}/C_n$  and  $\mathcal{X}/C_m$  are rational. In this paper, we provide a complete classification of such curves, as well as a characterization of their full automorphism groups.

## 1 Introduction

One of the leading problems of algebraic geometry is the classification of algebraic varieties. As most leading problems, it is largely unsolved. This holds true even if we restrict ourselves to 1-dimensional varieties, that is, algebraic curves. The essential tool in pursuing the goal of classifying (projective, nonsingular, geometrically irreducible, algebraic) curves is the study of their birational invariants, such as their genus and automorphism group. Since a general curve has trivial automorphism group, any curve  $\mathcal{X}$  with an automorphism group  $\text{Aut}(\mathcal{X}) \neq \{1\}$  is of particular interest. Further, curves equipped with a large automorphism group have a rich and interesting geometry. When the characteristic of the ground field  $\mathbb{K}$  is some prime  $p > 0$ , several exceptions to the classical Hurwitz bound for the order of  $\text{Aut}(\mathcal{X})$  are found, yielding classes of curves with particularly interesting properties. However, even in such exceptional cases, the automorphism group alone is not enough to characterize a curve, since Madden and Valentini [7] proved that for any finite group  $G$  there exists infinitely many non-isomorphic algebraic curves whose full automorphism group is isomorphic to  $G$ . Remarkably, in some cases it is possible to characterize a curve  $\mathcal{X}$  in terms of its automorphism group and genus. This happens for instance for the Hermitian curve, the Deligne-Lusztig-Suzuki curve and the Artin-Mumford curve; see [1, 4, 8].

Following this idea, one may ask which curves have a certain group  $G$  as a subgroup of  $\text{Aut}(\mathcal{X})$  with some extra condition on the action of  $G$  on the points of  $\mathcal{X}$ . The classification problem becomes even more challenging when considering curves defined over some finite field  $\mathbb{F}_q$  of order  $q = p^h$ . This case is also of interest in view of applications to Coding Theory and Finite Geometry.

In this paper, we classify all curves  $\mathcal{X}$  defined over a finite field  $\mathbb{F}_q$  of characteristic  $p > 2$  satisfying the following property:

- (P) The  $\mathbb{F}_q$ -automorphism group  $\text{Aut}_{\mathbb{F}_q}(\mathcal{X})$  of  $\mathcal{X}$  contains a subgroup  $G = C_n \times C_m$ , where  $C_i$  denotes a cyclic group of order  $i$  prime to  $p$ , such that  $\max\{n, m\} > 2$  and both quotient curves  $\mathcal{X}/C_n$  and  $\mathcal{X}/C_m$  are rational.

If  $n = m$  and the  $G$ -short orbits are  $\mathbb{F}_q$ -rational (that is, preserved by the  $\mathbb{F}_q$ -Frobenius automorphism  $\Phi_q$ ), a curve satisfying (P) is a generalized Fermat curve as introduced by Fanali and Giulietti in [2]. Thus, we will sometimes refer to a curve satisfying (P) as a generalized Fermat curve. It should be noted that the same term is used in the literature to describe similar yet rather different curves; see [2, 3].

As our main result, we provide the complete classification of the curves satisfying (P) and their full automorphism groups.

## 2 Background and preliminary results

Our notation and terminology are standard. Well-known references for the theory of curves and algebraic function fields are [4] and [9]. Let  $\mathcal{X}$  be a curve defined over some finite field  $\mathbb{F}_q$  of size  $q = p^h$  for some prime  $p$ ; then  $\mathcal{X}$  is viewed as a curve over the algebraic closure  $\mathbb{K}$  of  $\mathbb{F}_q$ . We denote by  $\mathbb{K}(\mathcal{X})$  the function field of  $\mathcal{X}$ . By a point  $P \in \mathcal{X}$  we mean a point in a nonsingular model of  $\mathcal{X}$ ; in this way, we have a one-to-one correspondence between points of  $\mathcal{X}$  and places of  $\mathbb{K}(\mathcal{X})$ . Let  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  denote the full automorphism group of  $\mathcal{X}$ . For a subgroup  $S$  of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ , we denote by  $\mathbb{K}(\mathcal{X})^S$  the fixed field of  $S$ . A nonsingular model  $\bar{\mathcal{X}}$  of  $\mathbb{K}(\mathcal{X})^S$  is referred as the quotient curve of  $\mathcal{X}$  by  $S$  and denoted by  $\mathcal{X}/S$ . Note that  $\mathcal{X}/S$  is defined up to birational equivalence. The field extension  $\mathbb{K}(\mathcal{X}) : \mathbb{K}(\mathcal{X})^S$  is Galois with Galois group  $S$ . For a point  $P \in \mathcal{X}$ ,  $S(P)$  is the orbit of  $P$  under the action of  $S$  on  $\mathcal{X}$  seen as a point-set. The orbit  $S(P)$  is said to be long if  $|S(P)| = |S|$ , short otherwise. There is a one-to-one correspondence between short orbits and ramified points in the extension  $\mathbb{K}(\mathcal{X}) : \mathbb{K}(\mathcal{X})^S$ . It might happen that  $S$  has no short orbits; if this is the case, the cover  $\mathcal{X} \rightarrow \mathcal{X}/S$  (or equivalently, the extension  $\mathbb{K}(\mathcal{X}) : \mathbb{K}(\mathcal{X})^S$ ) is unramified. On the other hand,  $S$  has a finite number of short orbits.

For  $P \in \mathcal{X}$ , the subgroup  $S_P$  of  $S$  consisting of all elements of  $S$  fixing  $P$  is called the stabilizer of  $P$  in  $S$ . For a non-negative integer  $i$ , the  $i$ -th ramification group of  $\mathcal{X}$  at  $P$  is denoted by  $S_P^{(i)}$ , and defined by

$$S_P^{(i)} = \{\sigma \mid v_P(\sigma(t) - t) \geq i + 1, \sigma \in S_P\},$$

where  $t$  is a local parameter at  $P$  and  $v_P$  is the respective discrete valuation. Here  $S_P = S_P^{(0)}$ . Furthermore,  $S_P^{(1)}$  is a normal  $p$ -subgroup of  $S_P^{(0)}$ , and the factor group  $S_P^{(0)}/S_P^{(1)}$  is cyclic of order prime to  $p$ ; see e.g. [4, Theorem 11.74]. In particular, if  $S_P$  is a  $p$ -group, then  $S_P = S_P^{(0)} = S_P^{(1)}$ .

Let  $g$  and  $\bar{g}$  be the genus of  $\mathcal{X}$  and  $\bar{\mathcal{X}} = \mathcal{X}/S$ , respectively. The Riemann-Hurwitz genus formula is

$$2g - 2 = |S|(2\bar{g} - 2) + \sum_{P \in \mathcal{X}} \sum_{i \geq 0} (|S_P^{(i)}| - 1); \quad (2.1)$$

see [4, Theorem 11.72]. If  $\ell_1, \dots, \ell_k$  are the sizes of the short orbits of  $S$ , then (2.1) yields

$$2g - 2 \geq |S|(2\bar{g} - 2) + \sum_{\nu=1}^k (|S| - \ell_\nu), \quad (2.2)$$

and equality holds if  $\gcd(|S_P|, p) = 1$  for all  $P \in \mathcal{X}$ ; see [4, Theorem 11.57 and Remark 11.61].

The following result (see [5, Proposition 1]) will be used in Section 6.

**Proposition 2.1** (Kontogeorgis). *Let  $\mathbb{F}_0$  be a rational function field over  $\mathbb{K}$ . Suppose that a cyclic extension  $\mathbb{F}$  of  $\mathbb{F}_0$  is completely ramified at  $s$  places and  $r = |\mathrm{Gal}(\mathbb{F} : \mathbb{F}_0)|$ . If  $2r < s$  then  $\mathrm{Gal}(\mathbb{F} : \mathbb{F}_0)$  is normal on the full automorphism group  $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$  of  $\mathbb{F}$ .*

Let  $\Phi_q : \mathcal{X} \rightarrow \mathcal{X}$  denote the  $\mathbb{F}_q$ -Frobenius map. An automorphism  $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$  is said to be  $\mathbb{F}_q$ -rational if it commutes with  $\Phi_q$ . A subgroup  $S$  of  $\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$  is  $\mathbb{F}_q$ -rational if every element of  $S$  commutes with  $\Phi_q$ . The subgroup of  $\mathrm{Aut}_{\mathbb{K}}(\mathcal{X})$  consisting of all  $\mathbb{F}_q$ -rational automorphisms is called the  $\mathbb{F}_q$ -automorphism group of  $\mathcal{X}$ , and it is denoted by  $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})$ . Note that  $\mathcal{X}/S$  is defined over  $\mathbb{F}_q$  for all  $S < \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})$ .

### 3 Cyclic subcovers of the projective line

The function field  $\mathbb{K}(\mathcal{C})$  of a rational curve  $\mathcal{C}$  is such that  $\mathbb{F} = \mathbb{K}(x)$  for some rational function  $x \in \mathbb{K}(\mathcal{C})$ . Since  $\mathcal{F}$  is birationally equivalent to  $\mathbb{P}^1(\mathbb{K})$ , we have that  $\mathrm{Aut}_{\mathbb{K}}(\mathcal{C}) \cong \mathrm{PGL}(2, \mathbb{K})$ . If  $\mathcal{C}$  is defined over  $\mathbb{F}_q$ , then  $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}) \cong \mathrm{PGL}(2, q)$ . We are interested in quotients of the projective line arising from tame cyclic subgroups of  $\mathrm{PGL}(2, q)$ ; by Dickson's Hauptsatz [10, Theorem 3], such groups have order  $k$  a divisor of  $q \pm 1$ .

Let  $\mathbb{F}$  be a rational function field over  $\mathbb{F}_q$ . Consider a cyclic extension  $\mathbb{F} : \mathbb{F}'$ , where  $\mathbb{F}'$  is a subfield of  $\mathbb{F}$  defined over  $\mathbb{F}_q$ . By Lüroth's Theorem,  $\mathbb{F}'$  is rational as well; see [9, Theorem 3.5.9].

**Proposition 3.1.** *Let  $\mathbb{F}$  be a rational function field over  $\mathbb{F}_q$ , where  $q = p^h$ , with  $p > 2$ . Let  $\mathbb{F}'$  be a subfield of  $\mathbb{F}$  such that the extension  $\mathbb{F} : \mathbb{F}'$  is cyclic of degree  $n$  prime to  $p$ , with  $n|q - 1$ . Assume that the ramified places of  $\mathbb{F} : \mathbb{F}'$  are  $\mathbb{F}_q$ -rational. Then there exists  $x \in \mathbb{F}$  such that  $\mathbb{F} = \mathbb{F}_q(x)$  and  $\mathbb{F}' = \mathbb{F}_q(x^n)$ .*

*Proof.* Let  $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F})$  be a generator of a cyclic subgroup of  $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F})$  of order  $n$ . Since  $n|q - 1$ , then  $\mathbb{F}_q$  has a  $n$ -th primitive root of the unity  $\zeta$ . There exists  $x \in \mathbb{F}$  with exactly one zero (and one pole)

defined over  $\mathbb{F}_q$  such that  $\sigma(x) = \zeta x$ . Then  $\sigma(x^n) = x^n$  holds. Clearly  $\mathbb{F} = \mathbb{F}_q(x)$ , whence our assertion follows.  $\square$

Now let us consider the case  $[\mathbb{F} : \mathbb{F}'] = n|q + 1$ . So let  $x \in \mathbb{F}$  such that  $\mathbb{F} = \mathbb{F}_q(x)$ , and let  $G$  be a cyclic subgroup of  $\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$  with  $|G| = n$  such that  $n|q + 1$ . Fix a nonsquare element  $s \in \mathbb{F}_q$  and define  $\mathbb{F}_{q^2}$  as an extension  $\mathbb{F}_q(i)$  of  $\mathbb{F}_q$  with  $i \in \mathbb{F}_{q^2}$  such that  $i^2 = s$ . Then  $\mathbb{F}_{q^2} = \{a + bi \mid a, b \in \mathbb{F}_q\}$ .

For  $\alpha = a + bi \in \mathbb{F}_{q^2}^*$ , set

$$M_\alpha = \begin{pmatrix} a & sb \\ b & a \end{pmatrix} \in \text{GL}(2, q).$$

The map  $\alpha \mapsto M_\alpha$  is a monomorphism from the multiplicative group  $\mathbb{F}_{q^2}^*$  to  $\text{GL}(2, q)$ . Let  $\lambda \in \mathbb{F}_{q^2}$  be a primitive  $(2n)$ -th root of the unity. Then the subgroup  $\langle M_\lambda \rangle$  of  $\text{GL}(2, q)$  is cyclic of order  $2n$ . The natural group homomorphism  $\varphi : \text{GL}(2, q) \rightarrow \text{PGL}(2, q)$  is surjective and  $\ker \varphi$  consists of all scalar matrices. Via a simple computation, one can show that  $\ker \varphi \cap \langle M_\lambda \rangle = \{M_1, M_{-1}\}$ . Hence  $\varphi$  maps  $\langle M_\lambda \rangle$  to a subgroup  $C$  of  $\text{PGL}(2, q)$  of order  $n$ . Note that the fixed points of  $C$  are  $(i : 1)$  and  $(-i : 1)$ . From the classification of subgroups of  $\text{PGL}(2, q)$  we know that there exists only one class of cyclic subgroups of order  $n$  fixing points not defined over  $\mathbb{F}_q$ <sup>1</sup>. Therefore, we have the following result.

**Proposition 3.2.** *Let  $G$  be a cyclic subgroup of  $\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_q(x))$  with  $|G| = n$  fixing no  $\mathbb{F}_q$ -rational place such that  $n|q + 1$ . Then, up to conjugacy,  $G = \langle \tau \rangle$ , where*

$$\tau(x) = \frac{ux + sv}{vx + u}, \quad (3.1)$$

with  $u + iv \in \mathbb{F}_{q^2}$  being a primitive  $(2n)$ -th root of the unity.

**Proposition 3.3.** *Let  $\mathbb{F}$  be a rational function field over  $\mathbb{F}_q$ , where  $q = p^h$ , with  $p > 2$ . Let  $\mathbb{F}'$  be a subfield of  $\mathbb{F}$  defined over  $\mathbb{F}_q$  such that the extension  $\mathbb{F} : \mathbb{F}'$  is cyclic of order  $n$  prime to  $p$  with no ramified  $\mathbb{F}_q$ -rational place, with  $n|q + 1$ . Then there exists  $x \in \mathbb{F}$  such that  $\mathbb{F} = \mathbb{F}_q(x)$  and  $\mathbb{F}' = \mathbb{F}_q(z)$  with  $z$  given by*

$$z = \frac{i[(x+i)^n - (x-i)^n]}{(x+i)^n + (x-i)^n}. \quad (3.2)$$

*Proof.* Let  $\tau \in \text{Aut}_{\mathbb{F}_q}(\mathbb{F})$  be such that  $\mathbb{F}' = \mathbb{F}^{\langle \tau \rangle}$ . Let  $x \in \mathbb{F}$  such that  $\mathbb{F} = \mathbb{F}_q(x)$  and  $\tau$  is defined on  $\mathbb{F}$  by (3.1). Consider the  $\mathbb{F}_{q^2}$ -rational function  $h(x)$  given by

$$h(x) = \frac{(x-i)^n}{(x+i)^n}. \quad (3.3)$$

A straightforward computation shows that  $\tau(h(x)) = \frac{(u-iv)^n(x-i)^n}{(u+iv)^n(x+i)^n} = h(x)$  as  $(u-iv)^n = (u+iv)^{qn} = (u+iv)^n$ . Then  $\mathbb{F}_{q^2}(h(x)) \subseteq \mathbb{F}_{q^2}(x)^{\langle \tau \rangle}$ . From  $n \leq [\mathbb{F}_{q^2}(x) : \mathbb{F}_{q^2}(h(x))] \leq n$  we get  $\mathbb{F}_{q^2}(h(x)) = \mathbb{F}_{q^2}(x)^{\langle \tau \rangle}$ . Let

---

<sup>1</sup>The only situation in which a cyclic subgroup of  $\text{PGL}(2, q)$  of order  $n|q + 1$  fixes an  $\mathbb{F}_q$ -rational point is  $n = 2$ .

$$z = i \cdot \frac{h(x) - 1}{h(x) + 1} = \frac{i[(x - i)^n - (x + i)^n]}{(x - i)^n + (x + i)^n}. \quad (3.4)$$

Then  $z \in \mathbb{F}_{q^2}(h(x)) \cap \mathbb{F}_q(x)$  with  $[\mathbb{F}_{q^2}(h(x)) : \mathbb{F}_{q^2}(z)] = 1$ , that is,  $\mathbb{F}' = \mathbb{F}_q(z)$ .  $\square$

**Remark 3.4.** Let  $\mathbb{F}$  and  $\mathbb{F}'$  as in Proposition 3.3. We may assume that  $\mathbb{F} = \mathbb{F}_q(x)$  and  $\mathbb{F}' = \mathbb{F}^{\langle \tau \rangle}$ , with  $\tau$  defined as in (3.1). It can be shown that  $\mathbb{F}' = \mathbb{F}_q(\text{Tr}(x))$ , where  $\text{Tr} : \mathbb{F} \rightarrow \mathbb{F}'$  is the trace map of the extension  $\mathbb{F} : \mathbb{F}'$ . In the same way, under the hypothesis of Lemma 3.1, let  $N : \mathbb{F} \rightarrow \mathbb{F}'$  denote the norm map of the extension  $\mathbb{F} : \mathbb{F}'$ . It can be shown that  $\mathbb{F} = \mathbb{F}_q(x)$  and  $\mathbb{F}' = \mathbb{F}_q(N(x))$  for some  $x \in \mathbb{F}$ .

We finish this section with a direct consequence of [10, Theorem 2].

**Lemma 3.5.** Let  $\mathcal{Y}$  be a rational curve defined over  $\mathbb{F}_q$ . Suppose that  $P$  is fixed by a subgroup  $C \subset \text{Aut}_{\mathbb{K}}(\mathcal{Y})$  of order  $n$  such that  $\gcd(p, n) = 1$ . If  $P$  is  $\mathbb{F}_q$ -rational, then  $C$  is cyclic and  $n|q - 1$ . If  $P$  is not  $\mathbb{F}_q$ -rational, then it is  $\mathbb{F}_{q^2}$ -rational and  $n|q + 1$ .

#### 4 Geometric properties of generalized Fermat curves

In this section, some geometric features of a curve  $\mathcal{X}$  satisfying property (P) are described. In particular, some results from [2, Section 3] are generalized.

**Lemma 4.1.** Let  $\mathcal{X}$  be a curve satisfying (P). Then  $m|q - 1$  or  $m|q + 1$ , and the same holds for  $n$ .

*Proof.* Since  $C_m$  normalizes  $C_n$ , there is a subgroup  $\tilde{C}_m$  of  $\text{Aut}_{\mathbb{F}_q}(\mathcal{X}/C_n)$  such that  $\tilde{C}_m \cong C_m$ . By  $\mathcal{X}/C_n \cong \mathbb{P}^1(\mathbb{F}_q)$ , it follows that  $\tilde{C}_m$  is isomorphic to a cyclic subgroup of  $\text{PGL}(2, q)$ . The result follows from [10, Theorem 3].  $\square$

**Lemma 4.2.** The function field  $\mathbb{F}_q(\mathcal{X})$  of  $\mathcal{X}$  is the compositum of  $\mathbb{F}_q(\mathcal{X}/C_n)$  and  $\mathbb{F}_q(\mathcal{X}/C_m)$ .

*Proof.* Set  $\mathbb{F} = \mathbb{F}_q(\mathcal{X}/C_n) \cdot \mathbb{F}_q(\mathcal{X}/C_m)$ . Since  $\mathbb{F}_q(\mathcal{X}/C_n) = \mathbb{F}_q(\mathcal{X})^{C_n}$  and  $\mathbb{F}_q(\mathcal{X}/C_m) = \mathbb{F}_q(\mathcal{X})^{C_m}$ , then the extension  $\mathbb{F}_q(\mathcal{X}) : \mathbb{F}$  is Galois with Galois group

$$\text{Gal}(\mathbb{F}_q(\mathcal{X}) : \mathbb{F}) = \text{Gal}(\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(\mathcal{X})^{C_n}) \cap \text{Gal}(\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(\mathcal{X})^{C_m}) = C_n \cap C_m = \{1\}.$$

Therefore  $\mathbb{F}_q(\mathcal{X}) = \mathbb{F}$ .  $\square$

We now present the main result of this section.

**Proposition 4.3.** Let  $\mathcal{X}$  be a curve of genus  $g$  satisfying (P). Denote by  $t$  the number of short orbits of  $G$ , and by  $\ell_1, \dots, \ell_t$  their sizes. Then  $m$  divides  $q - 1$  or  $q + 1$ ,  $n$  divides  $q - 1$  or  $q + 1$ , and one of the following holds:

$$(I) \quad t = 3, \ell_1 = m, \ell_2 = n, \ell_3 = \gcd(m, n), \text{ and } g = \frac{mn - m - n - \gcd(m, n) + 2}{2}.$$

(II)  $t = 4$ ,  $\ell_1 = \ell_2 = m$ ,  $\ell_3 = \ell_4 = n$ , and  $g = mn - m - n + 1$ .

*Proof.* It follows from Lemma 4.1 that  $m$  (and  $n$ ) divides  $q - 1$  or  $q + 1$ . By [10, Theorem 1], there are two distinct points  $P_1, P_2 \in \mathcal{X}/G$  that are fully ramified in the cover  $\mathcal{X}/C_n \rightarrow \mathcal{X}/G$ , and the remaining points of  $\mathcal{X}/G$  split completely in  $\mathcal{X}/C_n$ . Analogously, there are two distinct points  $Q_1, Q_2 \in \mathcal{X}/G$  (not necessarily distinct from  $P_1$  and  $P_2$ ) fully ramified in the cover  $\mathcal{X}/C_m \rightarrow \mathcal{X}/G$ , with the remaining points of  $\mathcal{X}/G$  splitting completely in  $\mathcal{X}/C_m$ . Since the cover  $\mathcal{X} \rightarrow \mathcal{X}/G$  is tame, Lemma 4.2 and Abhyankar's Lemma (see e.g. [9, Theorem 3.1.9]) imply that the possible sizes of a nontrivial one-point stabilizer in  $G$  are  $m$ ,  $n$  and  $\text{lcm}(m, n)$ . In other words, the possible sizes of the short orbits of  $G$  are  $m$ ,  $n$  and  $\text{gcd}(m, n)$ . Moreover, it also follows from Abhyankar's Lemma that a point-set  $\Omega \subset \mathcal{X}$  is a short orbit of  $G$  if and only if  $\Omega$  lie over  $P_i$  or  $Q_i$ ,  $i = 1, 2$ . In particular,  $2 \leq t \leq 4$ . Let  $t_1, t_2$ , and  $t_3$  be the number of short orbits of  $G$  of size  $n$ ,  $m$  and  $\text{gcd}(m, n)$ , respectively. Since  $\mathcal{X}/G$  is rational, the Riemann-Hurwitz formula (2.2) applied to the cover  $\mathcal{X} \rightarrow \mathcal{X}/G$  yields

$$2g - 2 = (t - 2)mn - t_1n - t_2m - t_3 \text{gcd}(m, n). \quad (4.1)$$

Suppose that  $t = 2$ . Then  $\{P_1, P_2\} = \{Q_1, Q_2\}$  and  $t_1 = t_2 = 0$ . By (4.1) we obtain that  $\text{gcd}(m, n) = 1$  and  $g = 0$ . Hence  $\mathcal{X}$  is a rational curve such that  $\text{Aut}_{\mathbb{F}_q}(\mathcal{X})$  has a subgroup isomorphic to  $C_n \times C_m$  with  $\text{gcd}(m, n) = 1$ , which is not allowed by the classification of the subgroups of  $\text{PGL}(2, q)$  ([10, Theorem 3]). Therefore,  $t \in \{3, 4\}$ .

Assume that  $t = 3$ . Then, without loss of generality,  $P_2 = Q_2$  and the short orbits of  $G$  lying over  $P_1$ ,  $P_2$  and  $Q_1$  have size  $n$ ,  $\text{gcd}(m, n)$  and  $m$ , respectively. Thus from (4.1) we have

$$g = \frac{mn - m - n - \text{gcd}(m, n) + 2}{2}.$$

Finally, assume that  $t = 4$ . Then  $\{P_1, P_2\} \cap \{Q_1, Q_2\} = \emptyset$ , the short orbits of  $G$  lying over  $P_1$  and  $P_2$  have size  $n$  and the short orbits of  $G$  lying over  $Q_1$  and  $Q_2$  have size  $m$ . Hence, by (4.1) we obtain  $g = mn - m - n + 1$ .  $\square$

## 5 Classification results

Let us recall that  $q = p^h$  with  $p > 2$  and  $m$  and  $n$  divide  $q \pm 1$ . In case that  $n$  (resp.  $m$ ) divides  $q + 1$ , we set the following notation. Fix a non-square  $s \in \mathbb{F}_q$  and choose a root  $i$  of the polynomial  $X^2 - s$ . Then  $\mathbb{F}_{q^2} = \{a_0 + ia_1 \mid a_0, a_1 \in \mathbb{F}_q\}$ . Our main result characterizes the curves satisfying property (P).

**Theorem 5.1.** *Let  $\mathcal{X}$  be a curve of genus  $g$  defined over  $\mathbb{F}_q$  satisfying (P). Denote by  $t$  the number of short orbits of  $G$ , and by  $\ell_1, \dots, \ell_t$  their sizes. Then one of the following holds:*

- (a)  $t = 3$ ,  $\ell_1 = m$ ,  $\ell_2 = n$ ,  $\ell_3 = \text{gcd}(m, n)$ , and  $g = \frac{mn - m - n - \text{gcd}(m, n) + 2}{2}$ . Furthermore, each short orbit of  $G$  is preserved by the  $\mathbb{F}_q$ -Frobenius map, both  $n$  and  $m$  divide  $q - 1$ , and  $\mathcal{X}$  is  $\mathbb{F}_q$ -birationally

equivalent to the curve defined by

$$aX^n + bY^m = 1, \quad (5.1)$$

where  $a, b \in \mathbb{F}_q^*$ .

(b)  $t = 4$ ,  $\ell_1 = \ell_2 = m$ ,  $\ell_3 = \ell_4 = n$ , and  $g = mn - m - n + 1$ . Moreover, one of the following occurs:

(b1) Each short orbit of  $G$  is preserved by the  $\mathbb{F}_q$ -Frobenius map, both  $n$  and  $m$  divide  $q - 1$ , and  $\mathcal{X}$  is  $\mathbb{F}_q$ -birationally equivalent to the curve defined by

$$aX^n Y^m + bX^n + cY^m = 1, \quad (5.2)$$

where  $a, b, c \in \mathbb{F}_q$  with  $c \neq \frac{a}{b}$  and  $a \neq 0$ .

(b2) Only two short orbit of  $G$  are preserved by the  $\mathbb{F}_q$ -Frobenius map, without loss of generality  $m|q - 1$  and  $n|q + 1$ , and  $\mathcal{X}$  is  $\mathbb{F}_q$ -birationally equivalent to the curve defined by

$$\frac{aY^m + b}{cY^m + d} = \frac{i[(X + i)^n - (X - i)^n]}{(X + i)^n + (X - i)^n}, \quad (5.3)$$

where  $a, b, c, d \in \mathbb{F}_q$ .

(b3)  $G$  has no short orbits preserved by the  $\mathbb{F}_q$ -Frobenius map, both  $n$  and  $m$  divide  $q + 1$ , and  $\mathcal{X}$  is  $\mathbb{F}_q$ -birationally equivalent to the curve defined by

$$\frac{[(ai + b)(X - i)^n + (b - ai)(X + i)^n][(Y - i)^m + (Y + i)^m]}{i[(ci + d)(X - i)^n + (d - bi)(X + i)^n][(Y - i)^m - (Y + i)^m]} = 1, \quad (5.4)$$

where  $a, b, c, d \in \mathbb{F}_q$ .

The proof of Theorem 5.1 will be obtained after a sequence of partial results. Henceforth, we denote by  $\pi_1 : \mathcal{X} \rightarrow \mathcal{X}/C_n$ ,  $\pi_2 : \mathcal{X} \rightarrow \mathcal{X}/C_m$  and  $\pi : \mathcal{X} \rightarrow \mathcal{X}/G$  the natural projections of  $\mathcal{X}$  onto the quotient curves  $\mathcal{X}/C_n$ ,  $\mathcal{X}/C_m$  and  $\mathcal{X}/G$  respectively. We will make use of the following fact.

**Lemma 5.2.** *Let  $z \in \mathbb{F}_q(\mathcal{X}/C_n)$ ,  $z' \in \mathbb{F}_q(\mathcal{X}/C_m)$  be such that  $\mathbb{F}_q(\mathcal{X}/C_n)^{C_m} = \mathbb{F}_q(z)$  and  $\mathbb{F}_q(\mathcal{X}/C_m)^{C_n} = \mathbb{F}_q(z')$ . Then there is  $\tau \in \text{PGL}(2, q)$  such that  $z' = \tau(z)$ .*

*Proof.* Clearly,  $\mathbb{F}_q(\mathcal{X})^G = (\mathbb{F}_q(\mathcal{X})^{C_m})^{C_n} = (\mathbb{F}_q(\mathcal{X})^{C_n})^{C_m}$ . Then  $\mathbb{F}_q(z) = \mathbb{F}_q(z')$ . □

**Lemma 5.3.** *Let  $\mathcal{X}$  be a curve defined over  $\mathbb{F}_q$ , where  $q = p^h$  ( $p > 2$ ), satisfying (P). Assume that  $G = C_n \times C_m$  has three short orbits in  $\mathcal{X}$ . Then each short orbit of  $G$  is preserved by the  $\mathbb{F}_q$ -Frobenius map. Moreover, both  $n$  and  $m$  divide  $q - 1$ .*

*Proof.* Recall that  $\Phi_q$  denotes the  $\mathbb{F}_q$ -Frobenius map. Since  $G$  is defined over  $\mathbb{F}_q$ , we have that  $\Phi_q$  acts on the set of orbits of  $G$ . As  $\Phi_q$  is bijective, it acts on the set of short orbits of  $G$ . Furthermore, since  $C_n$  and  $C_m$  are defined over  $\mathbb{F}_q$ , then  $\pi_i \circ \Phi_q = \Phi_q \circ \pi_i$  for  $i \in \{1, 2\}$ . Set  $\delta = \gcd(m, n)$  and let  $\Omega_1 = \{P_1^1, \dots, P_1^n\}$ ,

$\Omega_2 = \{P_2^1, \dots, P_2^\delta\}$  and  $\Omega_3 = \{P_3^1, \dots, P_3^m\}$  be the short orbits of  $G$ . The Riemann-Hurwitz formula (2.2) applied to the cover of curves  $\mathcal{X} \rightarrow \mathcal{X}/C_m$  yields

$$n(m-1) + (m-\delta) = \sum_{\nu=1}^k (m - \ell_\nu). \quad (5.5)$$

Since  $|\Omega_1| = n$ , the stabilizer in  $G$  of a point  $P_1^i \in \Omega_1$  has order  $m$ . Then, since  $\pi_2(\Omega_2)$  and  $\pi_2(\Omega_3)$  are over the only ramified points of  $\mathcal{X}/C_m \rightarrow \mathcal{X}/G$ , we conclude that  $C_m$  fixes  $\Omega_1$  elementwise. Also, from  $C_m$  preserving the  $\Omega_j$ , we obtain that  $\Omega_2$  forms a single orbit under  $C_m$ . From (5.5),  $C_m$  acts semi-regularly on the other points of  $\mathcal{X}$ . Thus  $\Phi_q(\sigma(P)) = \sigma(\Phi_q(P))$  for any  $P \in \mathcal{X}$  and  $\sigma \in C_m$  imply  $\phi_q(P_1^i) = \phi_q(P_1^j)$ , i.e.  $\Omega_1$  is  $\mathbb{F}_q$ -rational. The same argument applied to  $C_n$  shows that  $\Omega_3$  (and consequently  $\Omega_2$ ) is  $\mathbb{F}_q$ -rational. Now  $\pi_2(\Omega_3) \in \mathcal{X}/C_m$  is an  $\mathbb{F}_q$ -rational point and it is fully ramified in the cover  $\mathcal{X}/C_m \rightarrow \mathcal{X}/G$ . Therefore,  $n|q-1$  by Lemma 3.5. Since in the proof we can interchange the roles  $C_m$  and  $C_n$ , our claim follows.  $\square$

**Proposition 5.4.** *Let  $\mathcal{X}$  be a curve defined over  $\mathbb{F}_q$ , where  $q = p^h$  ( $p > 2$ ), satisfying (P). Assume that  $G = C_n \times C_m$  has three short orbits in  $\mathcal{X}$ . Then  $\mathcal{X}$  is  $\mathbb{F}_q$ -birationally equivalent to a curve defined by  $aX^n + bY^m = 1$ , with  $a, b \in \mathbb{F}_q^*$ .*

*Proof.* First, both  $n$  and  $m$  divide  $q-1$ , and the short orbits of  $G$  are  $\mathbb{F}_q$ -rational, by Lemma 5.3. Thus Lemma 3.1 implies that  $\mathbb{F}_q(\mathcal{X}/C_n) = \mathbb{F}_q(y)$ ,  $\mathbb{F}_q(\mathcal{X}/C_m) = \mathbb{F}_q(x)$  and  $\mathbb{F}_q(\mathcal{X}/G) = \mathbb{F}_q(y^m) = \mathbb{F}_q(x^n)$ , with  $x, y \in \mathbb{F}_q(\mathcal{X})$ . Moreover, it follows from Lemma 4.2 that  $\mathbb{F}_q(\mathcal{X}) = \mathbb{F}_q(x, y)$ . The extension  $\mathbb{F}_q(y) : \mathbb{F}_q(y^m)$  (resp.  $\mathbb{F}_q(x) : \mathbb{F}_q(x^n)$ ) has only two ramified points: the zero and the pole of  $y^m$  (resp.  $x^n$ ). Since each short orbit of  $G$  lie over only one of this points, we may assume (without loss of generality) that  $x^n$  and  $y^m$  have a common pole and distinct zeros. Therefore  $y^m = \alpha x^n + \beta$  for certain  $\alpha, \beta \in \mathbb{F}_q^*$ . The result then follows from the irreducibility of the last equation.  $\square$

**Lemma 5.5.** *Let  $\mathcal{X}$  be a curve defined over  $\mathbb{F}_q$ , where  $q = p^h$  ( $p > 2$ ), satisfying (P). Assume that  $G = C_n \times C_m$  has four short orbits in  $\mathcal{X}$ . Then one of the following holds:*

- (a) *Each short orbit of  $G$  is preserved by the  $\mathbb{F}_q$ -Frobenius map, and both  $n$  and  $m$  divide  $q-1$ .*
- (b) *Only two short orbit of  $G$  are preserved by the  $\mathbb{F}_q$ -Frobenius map,  $m|q-1$  and  $n|q+1$  (or vice-versa).*
- (c)  *$G$  has no short orbits preserved by the  $\mathbb{F}_q$ -Frobenius map, and both  $n$  and  $m$  divide  $q+1$ .*

*Proof.* Denote by  $\Omega_\iota$  the short orbits of  $G$ , where  $\iota \in \{1, 2, 3, 4\}$ . According to the proof of Proposition 4.3,  $\pi(\Omega_1) = P_1$ ,  $\pi(\Omega_2) = P_2$ ,  $\pi(\Omega_3) = Q_1$  and  $\pi(\Omega_4) = Q_2$ , with such points being pairwise distinct. Arguing as in the proof of Lemma 5.3, it can be shown that  $\Phi_q$  preserves the point-sets  $\Omega_1 \cup \Omega_2$  and  $\Omega_3 \cup \Omega_4$ . Since  $\Phi_q$  acts on the set of short orbits of  $G$ , we only have the following possibilities:



(a1) Each  $\Omega_i$  is preserved by  $\Phi_q$ .

(b1.1)  $\Phi_q$  preserves  $\Omega_1$  and  $\Omega_2$  and interchanges  $\Omega_3$  and  $\Omega_4$ .

(b1.2)  $\Phi_q$  preserves  $\Omega_3$  and  $\Omega_4$  and interchanges  $\Omega_1$  and  $\Omega_2$ .

(c1)  $G$  has no short orbits preserved by  $\Phi_q$ .

Set  $\overline{P}_1 := \pi_1(\Omega_1)$ ,  $\overline{P}_2 := \pi_1(\Omega_2)$ ,  $\overline{Q}_1 := \pi_2(\Omega_3)$  and  $\overline{Q}_2 := \pi_2(\Omega_4)$ . Suppose that (a1) holds. Then  $\overline{P}_1, \overline{P}_2 \in \mathcal{X}/C_n$  and  $\overline{Q}_1, \overline{Q}_2 \in \mathcal{X}/C_m$  are  $\mathbb{F}_q$ -rational points. Hence by Lemma 3.5 we obtain (a). In case (b1.1) holds, we have that  $\overline{P}_1, \overline{P}_2 \in \mathcal{X}/C_n$  are  $\mathbb{F}_q$ -rational, thus  $m|q-1$ . Furthermore, since  $\overline{Q}_1, \overline{Q}_2 \in \mathcal{X}/C_m$  are not  $\mathbb{F}_q$ -rational, it follows from Lemma 3.5 that  $n|q+1$ . Similarly, (b1.2) implies that  $n|q-1$  and  $m|q+1$ , thus we obtain (b). In view of the previous cases, (c) also follows from Lemma 3.5.  $\square$

**Proposition 5.6.** *Let  $\mathcal{X}$  be a curve defined over  $\mathbb{F}_q$ , where  $q = p^h$  ( $p > 2$ ), satisfying (P). Assume that  $G = C_n \times C_m$  has four short orbits in  $\mathcal{X}$ , each of them preserved by  $\Phi_q$ . Then  $\mathcal{X}$  is  $\mathbb{F}_q$ -birationally equivalent to a curve defined by  $aX^nY^m + bX^n + cY^m = 1$ , with  $a, b, c \in \mathbb{F}_q$  with  $c \neq \frac{a}{b}$  and  $a \neq 0$ .*

*Proof.* By Lemma 5.5(a), both  $n$  and  $m$  divide  $q-1$ , and the points  $\overline{P}_1, \overline{P}_2, \overline{Q}_1$  and  $\overline{Q}_2$  are  $\mathbb{F}_q$ -rational. Hence  $\mathbb{F}_q(\mathcal{X}/C_n) = \mathbb{F}_q(y)$ ,  $\mathbb{F}_q(\mathcal{X}/C_m) = \mathbb{F}_q(x)$  and  $\mathbb{F}_q(\mathcal{X}/G) = \mathbb{F}_q(y^m) = \mathbb{F}_q(x^n)$ , with  $x, y \in \mathbb{F}_q(\mathcal{X})$ , by Proposition 3.1. Hence

$$y^m = \frac{\alpha x^n + \beta}{\gamma x^n + \eta},$$

where  $\alpha, \beta, \gamma, \eta \in \mathbb{F}_q$  such that  $\alpha\eta \neq \beta\gamma$ . With notation as in Lemma 5.5, the points  $P_1, P_2, Q_1$  and  $Q_2$  are pairwise distinct. Here,  $\{P_1, P_2\}$  is the set of zero and pole of  $y^m$ , and  $\{Q_1, Q_2\}$  the set of zero and pole of  $x^n$ . Therefore,  $\beta$  and  $\gamma$  are nonzero. Thus, we have obtained an irreducible equation. The result now follows from Lemma 4.2.  $\square$

**Proposition 5.7.** *Let  $\mathcal{X}$  be a curve defined over  $\mathbb{F}_q$  satisfying (P). Assume that case (b) in Lemma 5.5 holds. Then  $\mathcal{X}$  is  $\mathbb{F}_q$ -birationally equivalent to curve defined by an affine equation*

$$\frac{aY^m + b}{cY^m + d} = \frac{i[(X+i)^n - (X-i)^n]}{(X+i)^n + (X-i)^n},$$

with  $a, b, c, d \in \mathbb{F}_q$  such that  $ad \neq bc$  and  $u + iv \in \mathbb{F}_{q^2}$  is an  $2n$ -th root of unity.

*Proof.* Without loss of generality, we can assume that  $m|q-1$  and  $n|q+1$ , with the points  $\overline{P}_1, \overline{P}_2 \in \mathcal{X}/C_n$  being  $\mathbb{F}_q$ -rational. The result then follows from Propositions 3.1, 3.3 and Lemmas 4.2 and 5.2.  $\square$

**Proposition 5.8.** *Let  $\mathcal{X}$  be a curve defined over  $\mathbb{F}_q$  satisfying (P). Assume that (c) in Lemma 5.5 holds. Then  $\mathcal{X}$  is  $\mathbb{F}_q$ -birationally equivalent to a curve defined by an affine equation*

$$\frac{[(ai+b)(X-i)^n + (b-ai)(X+i)^n][(Y-i)^m + (Y+i)^m]}{i[(ci+d)(X-i)^n + (d-bi)(X+i)^n][(Y-i)^m - (Y+i)^m]} = 1,$$

with  $a, b, c, d \in \mathbb{F}_q$ , with  $ad \neq bc$ .

*Proof.* Arguing as in the previous cases, the result follows from Proposition 3.3 and Lemmas 4.2 and 5.2.  $\square$

**Proof of Theorem 5.1** It follows by collecting the results from Propositions 4.3, 5.4, Lemma 5.5, Propositions 5.6, 5.7 and 5.8.  $\square$

**Remark 5.9.** Let  $\mathcal{X}$  be a curve satisfying (P). If we want to characterize  $\mathcal{X}$  up to birational equivalence over  $\mathbb{K}$ , then we have that either  $\mathcal{X}$  is  $\mathbb{F}_{q^2}$ -birationally equivalent to the curve defined by (5.1) or to the one defined by (5.2) (with the coefficients in  $\mathbb{F}_{q^2}$ ). Indeed, since the short orbits of  $G$  are preserved by  $\Phi_{q^2}$ , then  $m$  and  $n$  divide  $q \pm 1$  (Lemma 3.5), and so Proposition 3.1 applies to both extensions  $\mathbb{F}_{q^2}(\mathcal{X}/C_n) : \mathbb{F}_{q^2}(\mathcal{X}/G)$  and  $\mathbb{F}_{q^2}(\mathcal{X}/C_m) : \mathbb{F}_{q^2}(\mathcal{X}/G)$ .

**Remark 5.10.** It is possible that a curve defined by (5.2) admits a model given by an equation of type (5.1) for distinct powers of  $X$  and  $Y$ . Indeed, consider the hyperelliptic curve  $\mathcal{F}$  defined by the equation  $X^n Y^2 + X^n + Y^2 = 1$ . Then  $\mathcal{F}$  is  $\mathbb{F}_q$ -birationally equivalent to the curve defined by  $\bar{X}^{2n} + \bar{Y}^2 = 1$  via  $(X, Y) \mapsto (\bar{X}, \bar{Y}) := \left(X, \frac{2Y}{Y^2+1}\right)$ .

## 6 The full automorphism group

In this section, we exploit the full automorphism group of a curve  $\mathcal{X}$  defined over  $\mathbb{F}_q$  satisfying (P). Recall that  $\mathbb{K}$  denotes the algebraic closure of  $\mathbb{F}_q$ , where  $q = p^h$ . According to Theorem 5.1 and Remark 5.9, one of the following holds:

- (I)  $G = C_n \times C_m$  has 3 short orbits on  $\mathcal{X}$ , and  $\mathcal{X}$  is  $\mathbb{K}$ -birationally equivalent to the curve defined by  $X^n + Y^m = 1$ .
- (II)  $G = C_n \times C_m$  has 4 short orbits on  $\mathcal{X}$ , and  $\mathcal{X}$  is  $\mathbb{K}$ -birationally equivalent to the curve defined by  $aX^n Y^m + X^n + Y^m = 1$ , with  $a \in \mathbb{K}^*$ .

The full automorphism group  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  of the curves  $\mathcal{X}$  of case (I) above is completely characterized by Kontogeorgis [6], provided that  $p > 3$ ,  $m \neq n$ ,  $n \neq 4$  and  $m \neq 3$ . We summarize such characterization in the following Theorem.

**Theorem 6.1** (Kontogeorgis). *Let  $\mathcal{X}$  be a nonsingular model of the curve given by the affine equation  $X^n + Y^m = 1$ , where  $m < n$  with  $(m, n) \neq (3, 4)$ . Then  $C_m$  is a normal subgroup of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ , and*

$$\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong \begin{cases} C_n, & \text{if } m \nmid n; \\ D_n, & \text{if } m|n \text{ but } n-1 \text{ is not a power of } p; \\ \text{PGL}(2, p^r), & \text{if } m|n \text{ and } n-1 = p^r \text{ for some } r > 0. \end{cases}$$

If  $m = n$ , the case (I) provides the Fermat curve  $X^n + Y^n = 1$ . In this situation, it is well known that if  $n = p^r + 1$  for some  $r > 0$ , then  $\text{Aut}_{\mathbb{K}}(\mathcal{X}) \cong \text{PGU}(3, p^r)$  (see e.g. [4, Proposition 11.30]) and if  $n \neq p^r + 1$  for all  $r > 0$ , then  $C_n \times C_n$  is normal in  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  and  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/(C_n \times C_n) \cong S_3$  (see [4, Theorem 11.31]).

In view of such characterizations, in what follows in this section we assume that (II) above holds. Our main goal is to characterize  $\text{Aut}_{\mathbb{K}}(\mathcal{F})$ , where  $\mathcal{F} : aX^nY^m + X^n + Y^m = 1$ , where  $\max\{n, m\} > 2$ . Let  $\zeta_1, \zeta_2, c_1, c_2 \in \mathbb{K}$  such that  $\zeta_1$  (resp.  $\zeta_2$ ) is an  $n$ -th (resp.  $m$ -th) primitive root of the unity, and  $c_1^n = c_2^m = -a^{-1}$ . Let  $x$  and  $y$  such that  $\mathbb{K}(\mathcal{F}) = \mathbb{K}(x, y)$  and  $ax^n y^m + x^n + y^m = 1$ . From the equation of  $\mathcal{F}$ , one can see that  $\text{Aut}_{\mathbb{K}}(\mathcal{F})$  contains the following elements:

$$\sigma_1 : (x, y) \mapsto (\zeta_1 x, y), \quad \sigma_2 : (x, y) \mapsto (x, \zeta_2 y) \quad \text{and} \quad \mu : (x, y) \mapsto \left( \frac{c_1}{x}, \frac{c_2}{y} \right).$$

Here, we have  $C_n = \langle \sigma_1 \rangle$ ,  $C_m = \langle \sigma_2 \rangle$  and  $\mu$  is an involution that normalizes both  $C_n$  and  $C_m$ . Thus these three automorphisms generate a subgroup  $G \rtimes \langle \mu \rangle < \text{Aut}_{\mathbb{K}}(\mathcal{F})$  of order  $2mn$ . Moreover, since  $\mu \sigma_i \mu = \sigma_i^{-1}$  for  $i = 1, 2$ , we have that  $C_k \rtimes \langle \mu \rangle \cong D_k$ , where  $D_k$  denotes a dihedral group of order  $2k$ , with  $k \in \{m, n\}$ .

If  $a = 1$ , we can choose  $c_1$  (resp.  $c_2$ ) as a  $2n$ -th (resp.  $2m$ -th) primitive root of the unity. Hence  $\zeta_i = c_i^2$ , for  $i = 1, 2$ , and  $\text{Aut}_{\mathbb{K}}(\mathcal{F})$  contains

$$\tau_1 : (x, y) \mapsto \left( c_1 x, \frac{\zeta_2}{y} \right) \quad \text{and} \quad \tau_2 : (x, y) \mapsto \left( \frac{\zeta_1}{x}, c_2 y \right).$$

Note that  $\tau_i^2 = \sigma_i$  for  $i = 1, 2$ , but  $\tau_1 \tau_2 \neq \tau_2 \tau_1$ . Furthermore, if  $m = n$  we have the following extra involution

$$\theta : (x, y) \mapsto (y, x).$$

For convenience, from now on,  $\mathcal{X}$  stands for a nonsingular model of  $\mathcal{F}$ . In order to characterize the full automorphism group of  $\mathcal{X}$ , we will use the following results.

**Lemma 6.2.** *The group  $C_n \rtimes \langle \mu \rangle$  acts transitively on  $\Omega_1 \cup \Omega_2$ , and  $C_m \rtimes \langle \mu \rangle$  acts transitively on  $\Omega_3 \cup \Omega_4$ .*

*Proof.* Regarding  $\mathbb{K}(\mathcal{X})$  as a Kummer extension of the rational function fields  $\mathbb{K}(x)$  and  $\mathbb{K}(y)$ , it can be seen that, up to re-labeling the indices,

$$\text{div}(x) = \sum_{P \in \Omega_3} P - \sum_{Q \in \Omega_4} Q \quad \text{and} \quad \text{div}(y) = \sum_{R \in \Omega_1} R - \sum_{S \in \Omega_2} S.$$

More precisely,  $\Omega_1$  corresponds to  $\{(\zeta_1^k : 0 : 1) \mid 0 \leq k \leq n-1\}$  and  $\Omega_2$  consists of the points of  $\mathcal{X}$  centered at  $(0 : 1 : 0) \in \mathcal{F}$ , while  $\Omega_3$  corresponds to  $\{(0 : \zeta_2^s : 1) \mid 0 \leq s \leq m-1\}$  and  $\Omega_4$  is the set of points of  $\mathcal{X}$  centered at  $(1 : 0 : 0) \in \mathcal{F}$ . Clearly  $\sigma_1$  acts transitively on  $\Omega_1$  and  $\Omega_2$ , while  $\mu$  sends a zero of  $y$  on a pole of  $y$ , and vice-versa. Hence the first statement follows. The second is analogous.  $\square$

**Lemma 6.3.** *Assume that there exists  $\eta \in \text{Aut}_{\mathbb{K}}(\mathcal{X})$  such that  $\eta$  preserves the set of zeros and the set of poles of  $x$  and interchanges the set of zeros with the set of poles of  $y$ . Then  $a = 1$ .*

*Proof.* Since  $\eta$  preserves the set of zeros and the set of poles of  $x$ , then  $\text{div}(\eta(x)) = \text{div}(x)$ , which means that  $\eta(x) = \alpha x$  for some  $\alpha \in \mathbb{K}^*$ . In the same way,  $\eta$  interchanging the set of zeros with the set of poles of  $y$  gives that  $\text{div}(\eta(y)) = \text{div}(y^{-1})$ , and so  $\eta(y) = \frac{\beta}{y}$  for some  $\beta \in \mathbb{K}^*$ . Therefore, via the equation  $a\eta(x)^n\eta(y)^m + \eta(x)^n + \eta(y)^m = 1$ , we obtain  $(\alpha^n)x^ny^m + (a\alpha^n\beta^m)x^n - y^m + \beta^m = 0$ , which leads us to  $a = 1$ ,  $\alpha^n = -1$  and  $\beta^m = 1$ .  $\square$

### 6.1 The case $n \neq m$

We start our investigation with the case  $m \neq n$ . So, without loss of generality, assume that  $m < n$ . Following notation of the previous section, we know that  $G$  has 4 short orbits on  $\mathcal{X}$ , namely  $\Omega_1, \Omega_2, \Omega_3$  and  $\Omega_4$ , where  $\#(\Omega_1) = \#(\Omega_2) = n$  and  $\#(\Omega_3) = \#(\Omega_4) = m$ . Moreover,  $\Omega_1 \cup \Omega_2$  is the precise set of fixed points of  $C_m$  and  $\Omega_3 \cup \Omega_4$  is the precise set of fixed points of  $C_n$ . We begin from the following result.

**Lemma 6.4.** *Assume that  $m < n$ . Then  $C_m$  is a normal subgroup of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ .*

*Proof.* It follows directly from the above discussion and Proposition 2.1.  $\square$

Let  $f \geq h$  be the smallest integer such that  $\text{Aut}_{\mathbb{K}}(\mathcal{X}) = \text{Aut}_{\mathbb{F}_{p^f}}(\mathcal{X})$ . From Lemma 6.4, the full automorphism group of the quotient curve  $\mathcal{X}/C_m$  has a subgroup  $H$  defined over  $\mathbb{F}_{p^f}$  isomorphic to  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$ . Since  $\mathcal{X}/C_m$  is rational and defined over  $\mathbb{F}_{p^h}$ , we have  $\text{Aut}_{\mathbb{F}_{p^f}}(\mathcal{X}/C_m) \cong \text{PGL}(2, p^f)$ , and thus  $H$  has to be isomorphic to one of the groups in [10, Theorem 3]. Recall that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has always  $C_n \rtimes \langle \mu \rangle \cong D_n$  as a subgroup. Since such group meets  $C_m$  trivially, we conclude that  $H$  has a subgroup isomorphic to  $D_n$ . With this on hands, we are able to prove the following.

**Theorem 6.5.** *Assume that  $m < n$ , with  $n \neq 4$ . If  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has no  $p$ -subgroup, then*

$$\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong \begin{cases} D_{2n}, & \text{if } a = 1, \\ D_n, & \text{if } a \neq 1. \end{cases}$$

*Proof.* Since  $D_n < \text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$ , by [10, Theorem 3]  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$  is isomorphic to one of the following groups:  $D_\ell$  with  $\ell | p^f \pm 1$ ,  $S_4$  and  $A_5$  (the remaining groups in the Hauptsatz [10, Theorem 3]). Note that, since the point-set  $\Omega_1 \cup \Omega_2 \subset \mathcal{X}$  is the precise set of fixed points of  $C_m$ , Lemma 6.2 gives that  $\Omega_1 \cup \Omega_2$  is a short orbit of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ . Assume that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong A_5$ . Then, since  $D_5$  is the unique dihedral subgroup of  $A_5$ , we obtain  $n = 5$ . Moreover,  $|\text{Aut}_{\mathbb{K}}(\mathcal{X})| = 60m$ , and by the Orbit-Stabilizer Theorem, the stabilizer of a point  $P \in \Omega_1 \cup \Omega_2$  in  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has size  $6m$ . Hence, the stabilizer of  $\pi_2(P) \in \mathcal{X}/C_m$  in  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$  has size 6. Thus, [10, Theorem 1] provides that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has only two short orbits: one of size 10 and one of size  $12m$ . Then, by Riemann-Hurwitz formula (2.2) applied to the cover  $\mathcal{X} \rightarrow \mathcal{X}/\text{Aut}_{\mathbb{K}}(\mathcal{X})$ , we

obtain  $m = 0$ , a contradiction. Thus  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \not\cong A_5$ . We also have  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \not\cong S_4$ , from  $D_4$  being the unique dihedral subgroup of  $S_4$ , which implies  $n = 4$ .

Therefore,  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong D_\ell$  for some  $\ell$ . From the normality of  $C_m$ , there exists  $\bar{C}_n < \text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$  such that  $\bar{C}_n \cong C_n$ . In particular,  $n|\ell$ . Since  $\Omega_3 \cup \Omega_4$  is pointwise fixed by  $C_n$ , both points  $\pi_2(\Omega_3), \pi_2(\Omega_4) \in \mathcal{X}/C_m$  are fixed by  $\bar{C}_n$ . Thus from [10, Theorem 1] it follows that all the points of  $(\mathcal{X}/C_m) \setminus \{\pi_2(\Omega_3), \pi_2(\Omega_4)\}$  are in long orbits of  $\bar{C}_\ell$ , where  $\bar{C}_\ell$  is the cyclic normal subgroup of  $D_\ell$ . Hence the set  $\pi_2(\Omega_1 \cup \Omega_2)$  is an union of long orbits of  $\bar{C}_\ell$ . Therefore, since  $\#(\pi_2(\Omega_1 \cup \Omega_2)) = \#(\Omega_1 \cup \Omega_2) = 2n$ , we conclude that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong D_\ell$ , with  $\ell \in \{n, 2n\}$ . We will proceed to prove that  $\ell = 2n$  if and only if  $a = 1$ . If  $a = 1$ , we have defined on  $\mathcal{X}$  the automorphism  $\tau_1 : (x, y) \mapsto (c_1 x, \frac{c_2}{y})$ . The group  $\langle \tau_1 \rangle$  is cyclic of order  $2n$ , and it meets  $C_m$  trivially. Thus  $\langle \tau_1 \rangle \cong \bar{C}_\ell$  and  $\ell = 2n$ . Assume now that  $\ell = 2n$ . As before, denote by  $\bar{C}_\ell$  the cyclic subgroup of  $D_\ell$  of order  $\ell$ . Let  $\bar{\delta}$  such that  $\langle \bar{\delta} \rangle = \bar{C}_\ell$  and consider  $\delta \in \text{Aut}_{\mathbb{K}}(\mathcal{X})$  such that  $\bar{\delta}$  is the image of  $\delta$  under the natural group projection of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  onto  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$ . On one hand, since  $\bar{\delta}$  acts transitively on  $\pi_2(\Omega_1 \cup \Omega_2)$  and  $\bar{\delta}^2$  acts transitively on both  $\pi_2(\Omega_1)$  and  $\pi_2(\Omega_2)$ , we see that  $\bar{\delta}$  gives an injection from  $\pi_2(\Omega_1)$  onto  $\pi_2(\Omega_2)$ . Thus  $\delta$  maps bijectively the set of zeros onto the set of poles of  $y$ . On the other hand,  $\bar{\delta}$  fixes both  $\pi_2(\Omega_3), \pi_2(\Omega_4) \in \mathcal{X}/C_m$ , whence  $\delta$  preserves both  $\Omega_3$  and  $\Omega_4$ . In other words,  $\delta$  preserves the set of zeros and the set of poles of  $x$ . Hence the result follows from Lemma 6.3.  $\square$

Now we study the case in which  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a  $p$ -subgroup. We start by pointing out that  $\mathcal{X}$  can have automorphisms of order  $p$ .

**Lemma 6.6.** *Let  $\mathcal{X}$  be a nonsingular model of the hyperelliptic curve defined over  $\mathbb{K}$  by the equation  $X^n Y^2 + X^n + Y^2 = 1$ , where  $n = \frac{p^r+1}{2}$  for some  $r > 0$ . Then  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_2 \cong \text{PGL}(2, p^r)$ .*

*Proof.* Remark 5.10 implies that  $\mathcal{X}$  has a plane model defined by  $\bar{X}^{p^r+1} + \bar{Y}^2 = 1$ . Therefore, the result follows from Theorem 6.1.  $\square$

**Lemma 6.7.** *Assume that  $m < n$  and that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a  $p$ -subgroup of order  $p^r$ , with  $r > 0$ . Then such  $p$ -group has a single fixed point  $P \in \mathcal{X}$  such that  $P \in \Omega_1 \cup \Omega_2$ , and it acts semi-regularly on the remaining points of  $\mathcal{X}$ . Furthermore,  $p^r | 2n - 1$ .*

*Proof.* Assume that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a subgroup  $E$  of order  $p^r$ . Since  $p \nmid m$ , we have that  $E$  meets  $C_m$  trivially, and thus by [10, Theorem 3] there is an elementary abelian  $p$ -group  $E_{p^r} < \text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$  isomorphic to  $E$  (in particular,  $E$  must be abelian). From [10, Theorem 1], the group  $E_{p^r}$  fixes only one point and acts semi-regularly on the remaining points of  $\mathcal{X}/C_m$ . By the normality of  $C_m$ , we see that  $E_{p^r}$  acts on the points of  $\mathcal{X}/C_m$  as  $E$  does on the set of orbits of  $C_m$  on  $\mathcal{X}$ . Since  $\Omega_1 \cup \Omega_2$  is the precise set of fixed points of  $C_m$ , this means that  $E(\Omega_1 \cup \Omega_2) = \Omega_1 \cup \Omega_2$ , and thus  $E_{p^r}(\Gamma) = \Gamma$ , where  $\Gamma = \pi_2(\Omega_1 \cup \Omega_2)$ . So let  $Q \in \mathcal{X}/C_m$  be the unique fixed point of  $E_{p^r}$ . If  $Q \notin \Gamma$ , then  $\Gamma$  would be a union of long orbits of  $E_{p^r}$ , whence  $p^r | \#(\Gamma) = 2n$ , a contradiction. Therefore,  $Q \in \Gamma$ , whence  $P := \pi_2^{-1}(Q) \in \Omega_1 \cup \Omega_2$  is the only fixed point of  $E$ . In addition,  $\Gamma \setminus \{Q\}$  is a union of long orbits of  $E_{p^r}$ , which finishes the proof.  $\square$

**Proposition 6.8.** *Assume that  $m < n$  and that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a Sylow  $p$ -subgroup of order  $p^r$ , with  $r > 0$ . Then  $\text{PSL}(2, p^r) < \text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$  and  $n = \frac{p^r+1}{2}$ .*

*Proof.* From [10, Theorem 3],  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$  is isomorphic either to  $\text{PSL}(2, p^r)$  or to  $\text{PGL}(2, p^r)$ , with  $r|f$ . In any case,  $\text{PSL}(2, p^r) < \text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$ . So, on one hand, since  $p \nmid m$ , we have that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a subgroup  $E \cong E_{p^r}$ . Thus Lemma 6.7 gives us that  $p^r|2n-1$ . On the other hand, [10, Theorem 3] implies that  $n|p^r \pm 1$ . If  $n|p^r - 1$ , we would have integers  $s_1, s_2 > 0$  such that  $2n - 1 = s_1 p^r$  and  $p^r - 1 = s_2 n$ . Then  $(2 - s_1 s_2)p^r = s_2 + 2$ , which is only possible for  $s_1 = s_2 = 1$  and  $p^r = 3$ , and so  $n = 2$  and  $m = 1$ , a contradiction. If  $n|p^r + 1$ , as in the previous case, write  $2n - 1 = s_1 p^r$  and  $p^r + 1 = s_2 n$ , with integers  $s_1, s_2 > 0$ . Thus  $(2 - s_1 s_2)p^r = s_2 - 2$ , which is only possible for  $s_1 = 1$  and  $s_2 = 2$ . Then  $n = \frac{p^r+1}{2}$ .  $\square$

**Proposition 6.9.** *Assume that  $m < n$  and that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a Sylow  $p$ -subgroup  $E$  of order  $p^r$ , with  $r > 0$ . Then the quotient curve  $\mathcal{X}/E$  is rational.*

*Proof.* By Proposition 6.8, there exists  $W < \text{Aut}_{\mathbb{K}}(\mathcal{X})$  such that  $W/C_m \cong \text{PSL}(2, p^r)$ . Moreover, since  $n = \frac{p^r+1}{2}$ , one can check that  $C_n < W$ . From [10, Theorem 1],  $\text{PSL}(2, p^r)$  has two short orbits on  $\mathcal{X}/C_m$ , a non-tame one, which we denote by  $\Gamma_1$ , and a tame one, denoted by  $\Gamma_2$ . Moreover,  $\#(\Gamma_1) = p^r + 1 = 2n$  and  $\#(\Gamma_2) = p^r(p^r - 1)$ . Set  $\Lambda_1 = \Omega_1 \cup \Omega_2 \subset \mathcal{X}$ . Each point of  $\Lambda_1$  is fully ramified in the cover  $\mathcal{X} \rightarrow \mathcal{X}/C_m$ , and the remaining points of  $\mathcal{X}$  have trivial stabilizer in  $C_m$ . By Lemma 6.7, there is a point  $P_1 \in \Lambda_1$  fixed by  $E$ , and  $E$  acts transitively on  $\mathcal{X} \setminus \{P_1\}$ ; in particular,  $E = W_{P_1}^{(1)}$ . Since  $C_m < W_{P_1}$  and  $p \nmid m$ , the point  $\pi_2(P_1) \in \mathcal{X}/C_m$  has a non-tame stabilizer. Thus  $\pi_2(P_1) \in \Gamma_1$ . By the normality of  $C_m$ ,  $\text{PSL}(2, p^r)$  acts on the points of  $\mathcal{X}/C_m$  as  $W$  does on the set of orbits of  $\mathcal{X}$ . Hence,  $\Lambda_1$  is a short orbit of size  $2n$  of  $W$ . Now let  $Q_1 \in \Omega_3 \cup \Omega_4$ . Since  $C_n$  fixes  $\Omega_3 \cup \Omega_4$  pointwise, we have that  $\pi_2(Q_1) \in \mathcal{X}/C_m$  has nontrivial stabilizer. Since  $\pi_2(Q_1) \notin \Gamma_1$ , we have that  $\pi_2(Q_1) \in \Gamma_2$ , and so its stabilizer on  $\text{PSL}(2, p^r)$  is tame, and by [10, Theorem 1] it has size  $n$ . The same holds for  $\pi_2(Q_4)$ . Therefore, from the fact that every point of  $\mathcal{X}$  outside  $\Lambda_1$  has trivial stabilizer on  $C_m$ , we see that  $W$  has another short orbit  $\Lambda_2$  (containing  $\Omega_3 \cup \Omega_4$ ) on  $\mathcal{X}$  of size  $mp^r(p^r - 1)$ , and  $\Lambda_1$  and  $\Lambda_2$  are the only short orbits of  $W$ . Thus, recalling that  $\mathcal{X}/C_m$  is rational and  $|\text{PSL}(2, p^r)| = p^r(p^r - 1)n$ , the Riemann-Hurwitz formula (2.1) applied to the cover  $\mathcal{X} \rightarrow \mathcal{X}/W$  gives

$$2mn - 2m - 2n = -2mnp^r(p^r - 1) + mp^r(p^r - 1)(|W_{Q_1}| - 1) + 2n(|W_{P_1}| - 1) + 2n \sum_{i \geq 1} (|W_{P_1}^{(i)}| - 1),$$

and so

$$2mn - 2m - 2n = -2mnp^r(p^r - 1) + mp^r(p^r - 1)(n - 1) + 2n \left( \frac{m(p^r - 1)p^r}{2} + p^r - 2 \right) + 2n \sum_{i \geq 2} (|W_{P_1}^{(i)}| - 1),$$

which gives

$$\sum_{i \geq 2} (|W_{P_1}^{(i)}| - 1) = (m - 1)(p^r - 1). \quad (6.1)$$

Now, denote by  $\tilde{g}$  the genus of  $\mathcal{X}/E$ . From  $\{P_1\}$  being the unique short orbit of  $E$ , the Riemann-Hurwitz formula (2.1) applied to  $\mathcal{X} \rightarrow \mathcal{X}/E$  provides

$$2mn - 2m - 2n = 2p^r(\tilde{g} - 1) + 2p^r - 2 + \sum_{i \geq 2} (|E_{P_1}^{(i)}| - 1).$$

Hence

$$\tilde{g} = \frac{(m-1)(p^r-1) - \sum_{i \geq 2} (|E_{P_1}^{(i)}| - 1)}{2p^r}. \quad (6.2)$$

The result now follows from (6.1), (6.2) and from the equality  $E = W_{P_1}^{(1)}$ .  $\square$

Let  $x, y \in \mathbb{K}(\mathcal{X})$  such that  $\mathbb{K}(x, y) = \mathbb{K}(\mathcal{X})$  and  $ax^ny^m + x^n + y^m = 1$ . If  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  contains a Sylow  $p$ -subgroup  $E$  of order  $p^r$ , then  $\mathcal{X}/E$  is rational and  $\mathcal{X}$  has a point  $P_1$  that is the unique point fixed by  $E$ . Moreover,  $P_1 \in \Omega_1 \cup \Omega_2$ , and so there is  $\lambda \in \mathbb{K}^*$  such that  $\text{div}((x - \lambda)^{-1})_{\infty} = mP_1$ . Furthermore, thanks to the proof of Theorem 6.9, we know that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has no fixed points. Finally,  $2n = p^r + 1$  and  $g = (n-1)(m-1)$ . Therefore, via [4, Theorem 12.4 and Theorem 12.11], we have the following.

**Proposition 6.10.** *Assume that  $m < n$  and that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a Sylow  $p$ -subgroup  $E$  of order  $p^r$ , with  $r > 0$ . Then:*

- $\mathbb{K}(\mathcal{X}) = \mathbb{K}(z, w)$ , where  $z^{p^r} + z = w^m$ , with  $p^r \equiv -1 \pmod{m}$  and  $P_1$  is the common pole of  $z$  and  $w$ ;
- $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong \text{PGL}(2, p^r)$ ;
- $C_m$  fixes each of the  $p^r + 1$  points with the same Weierstrass semigroup as  $P_1$ ;
- $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$  acts on the set of such  $p^r + 1$  points as  $\text{PGL}(2, p^r)$ .

**Theorem 6.11.** *Assume that  $m < n$  and that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a Sylow  $p$ -subgroup of order  $p^r$ . Then  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong \text{PGL}(2, p^r)$ ,  $a = 1$ ,  $n = \frac{p^r+1}{2}$  and  $m = 2$ .*

*Proof.* The first statement follows from Proposition 6.10. We keep the notation of the proof of Proposition 6.9. Arguing as in the proof of such Proposition, we see that  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has only two short orbits:  $\Lambda_1 = \Omega_1 \cup \Omega_2$ , that has size  $2n$ , and  $\Lambda_2$ , of size  $mp^r(p^r - 1)$ . Let  $Q_1 \in \Omega_3 \cup \Omega_4 \subset \Lambda_2$ . From Proposition 6.10, we obtain that the stabilizer  $(\text{Aut}_{\mathbb{K}}(\mathcal{X}))_{Q_1}$  of  $Q_1$  is a cyclic group of order  $2n$  that acts transitively on  $\Lambda_1$ . Thus Lemma 6.3 implies that  $a = 1$ . Moreover,  $(\text{Aut}_{\mathbb{K}}(\mathcal{X}))_{Q_1} = \langle \tau_1 \rangle$ . The group  $\langle \tau_1 \rangle$  is, up to conjugacy, the only cyclic group of order  $2n$  fixing a point of  $\mathcal{X}$ . This happens because no such group is in the stabilizer  $(\text{Aut}_{\mathbb{K}}(\mathcal{X}))_P$  of some point  $P \in \Lambda_1$ , since  $|(\text{Aut}_{\mathbb{K}}(\mathcal{X}))_P| = mp^r(p^r - 1) = 2m(2n - 1)(n - 1)$ . Hence every cyclic group of order  $2n$  fixing a point is the stabilizer of some point  $Q \in \Lambda_2$ , whence conjugated to  $\langle \tau_1 \rangle$ . Furthermore,  $C_m$  is the only cyclic normal subgroup of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  of order  $\geq m$ . Indeed, the existence of a cyclic normal subgroup  $T \neq C_m$  of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  would imply the existence of a cyclic normal subgroup  $\bar{T}$  of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong \text{PGL}(2, p^r)$ , a contradiction.

Now let  $\varepsilon, \kappa \in \mathbb{K}$  such that  $\varepsilon^{p^r+1} = -1$  and  $\kappa^{p^r} + \kappa = 1$ . Then  $\mathbb{K}(u, v) = \mathbb{K}(z, w)$ , where  $u = \frac{\varepsilon}{z-\kappa} + \varepsilon$  and  $v = w \left( \frac{\varepsilon}{z-\kappa} \right)^{\frac{p^r+1}{m}}$ . Note that  $v^m = u^{p^r+1} + 1$ . In other words,  $\mathcal{X}$  is birationally equivalent to the curve  $\mathcal{C}$  defined by the affine equation  $X_1^{2n} + X_2^n = 1$ . Denote by  $K_{2n}$  the group generated by the automorphism  $\phi_1 : (u, v) \mapsto (c_1 u, v)$  and by  $K_m$  the group generated by  $\phi_2 : (u, v) \mapsto (u, \zeta_2 v)$ . It should be noted that  $\phi_1$  and  $\phi_2$  commute. The group  $K_m$  fixes  $2n$  points of  $\mathcal{X}$  (this was shown in the proof of Lemma 5.3, since  $K_{2n} \times K_m$  has three short orbits on  $\mathcal{X}$ ). Thus  $K_m$  is a normal subgroup of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ , by Theorem 2.1. Therefore,  $K_m = C_m$ . On its turn,  $K_{2n}$  also has fixed points on  $\mathcal{X}$ , by the same reasons that  $K_m$  does. Hence  $K_{2n} = \sigma C_{2n} \sigma^{-1}$  for some  $\sigma \in \text{Aut}_{\mathbb{K}}(\mathcal{X})$ . But  $C_m$  is a normal subgroup of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  and  $\sigma_2$  commutes with  $\phi_1$ . Thus  $\sigma_2$  commutes with  $\tau_1$ . In particular,  $\tau_1 \sigma_2(y) = \frac{\zeta_2^2}{y}$  and  $\sigma_2 \tau_1(y) = \frac{1}{y}$ . Therefore  $\zeta_2^2 = 1$ , which means that  $m = 2$ . This finishes the proof.  $\square$

**Theorem 6.12.** *Let  $\mathcal{X}$  be a nonsingular model of the curve defined over the algebraic closure  $\mathbb{K}$  of  $\mathbb{F}_q$  by the equation  $aX^n Y^m + X^n + Y^m = 1$ , where  $m < n$  and  $p \nmid mn$ . Assume that  $n \neq 4$ . Then  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  has a normal cyclic subgroup  $C_m$  of order  $m$ , and*

$$\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m \cong \begin{cases} D_n, & \text{if } a \neq 1; \\ D_{2n}, & \text{if } a = 1 \text{ and } (m, n) \neq \left(2, \frac{p^r+1}{2}\right) \text{ for all } r > 0; \\ \text{PGL}(2, p^r) & \text{if } a = 1 \text{ and } (m, n) = \left(2, \frac{p^r+1}{2}\right) \text{ for some } r > 0. \end{cases} \quad (6.3)$$

*Proof.* This follows from Theorems 6.5 and 6.11.  $\square$

**Remark 6.13.** *Let  $H = \text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m$  and  $s = |\text{Aut}_{\mathbb{K}}(\mathcal{X})/C_m|$ . If  $\gcd(m, s) = 1$ , then  $\text{Aut}_{\mathbb{K}}(\mathcal{X}) \cong C_m \rtimes H$  by the Schur-Zassenhaus Theorem. If  $\gcd(m, s) \neq 1$ , it might happen that  $C_m$  has no complement in  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ .*

## 6.2 The case $n = m$

If  $n = m$ , a different approach for the determination of the full automorphism group of  $\mathcal{X}$  is needed. Henceforth,  $\mathcal{X}$  is a nonsingular model of  $\mathcal{F} : aX^m Y^m + X^m + Y^m = 1$ , where  $a \in \mathbb{K}^*$ .

**Lemma 6.14.** *The set  $\Omega = \Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$  is an  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ -short orbit of size  $4m$ .*

*Proof.* First, note that  $\Omega$  is a unique orbit under the action of the group generated by  $C_m \times C_m$ ,  $\theta$  and  $\mu$  since  $\theta(\Omega_1) = \Omega_3$  and  $\theta(\Omega_2) = \Omega_4$  while  $\mu(\Omega_1) = \Omega_2$  and  $\mu(\Omega_3) = \Omega_4$ . Also, it is immediately seen that  $m$  is a non-gap at any point lying on  $\Omega$ . Next, we show that  $m$  is a gap number at any point  $O \notin \Omega$ , is centered at  $U = (b : c : 1) \in \mathcal{F}$  with  $b, c \neq 0$ . Let  $\ell$  be the tangent line to  $\mathcal{F}$  at  $U$ . It can be straightforwardly checked that  $U$  is not an inflection point of  $\mathcal{F}$ , from where the intersection multiplicity  $I(U, \mathcal{F} \cap \ell) = 2$ . Then the curve  $\mathcal{C}$  having the vertical line  $X - a$  counted  $m - 3$  times, the line  $Z = 0$  counted  $m - 1$  times and  $\ell$  as components is a canonical adjoint for  $\mathcal{X}$  such that  $I(U, \mathcal{F} \cap \mathcal{C}) = m - 1$ . This implies that  $m$  is a gap number at  $O$ .  $\square$



**Lemma 6.15.** *Let  $\Omega_1 = \{R_1, \dots, R_m\}, \Omega_2 = \{S_1, \dots, S_m\}, \Omega_3 = \{P_1, \dots, P_m\}, \Omega_4 = \{Q_1, \dots, Q_m\}$ . For  $i, j, h, k$  such that  $i + j + h + k = m$ , consider the divisor*

$$D := P_1 + \dots + P_i + Q_1 + \dots + Q_j + R_1 + \dots + R_h + S_1 + \dots + S_k.$$

*Then the linear series  $|D|$  has projective dimension*

$$\dim |D| = \begin{cases} 1, & \text{if } l = m \text{ for some } l \in \{i, j, h, k\}; \\ 0, & \text{otherwise.} \end{cases}$$

*Proof.* For the first part of the assertion, without loss of generality we may assume  $i = m$ , i.e.  $D = P_1 + \dots + P_m$ . Recall that any linear series is cut out on  $\mathcal{F}$  by the adjoints of some degree  $s$ . Since  $\mathcal{F}$  has only ordinary  $m$ -fold singularities at  $(0 : 1 : 0)$  and  $(1 : 0 : 0)$ , a curve  $\mathcal{C}$  of degree  $s$  is an adjoint for  $\mathcal{F}$  if and only if  $\mathcal{C}$  has at least an  $(m-1)$ -th fold point at each of these points. The degree  $m$  curve  $\mathcal{C} : XZ^{m-1} = 0$  is such that the intersection divisor  $\mathcal{C} \cdot \mathcal{F} = P_1 + \dots + P_m + m(S_1 + \dots + S_m) + (m-1)(Q_1 + \dots + Q_m)$ . Hence, the linear series  $|D|$  is cut out on  $\mathcal{F}$  by all the curves of degree  $m$  intersecting  $\mathcal{F}$  at least  $m$  times in each of the  $S_h$ 's and at least  $(m-1)$  times at each of the  $Q_j$ 's. Since all such curves are of the type  $a_1 XZ^{m-1} + a_2 Z^m = 0$ , our assertion follows. For the second part, without loss of generality we may assume that the support of  $D$  is contained in  $\Omega_1 \cup \Omega_3$ . Then arguing as in the previous case, it is easily seen that the linear series  $|D|$  in this case is cut out on  $\mathcal{F}$  by all the curves of degree  $m+1$  passing through  $P_{i+1}, \dots, P_m, R_{j+1}, \dots, R_m$  and at least  $m-1$  times at each of the  $Q_j$ 's and  $S_h$ 's. Since there is just one curve satisfying such condition, namely  $\mathcal{G} : XYZ^{m-1} = 0$ , our assertion follows.  $\square$

**Proposition 6.16.**  *$\text{Aut}_{\mathbb{K}}(\mathcal{X})$  admits a representation as a permutation group on the set  $\{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$ .*

*Proof.* By contradiction, assume there exists  $\alpha \in \text{Aut}_{\mathbb{K}}(\mathcal{X})$  which does not permute the  $\Omega_i$ 's. Let  $D = P_1 + \dots + P_m$ . Then the support of  $\alpha(D)$  is contained in more than one of the short orbits  $\Omega_i$ . In particular,  $1 = \dim(|D|) = \dim(|\alpha(D)|)$ , a contradiction by Lemma 6.15.  $\square$

**Theorem 6.17.** *If  $n = m$ , then  $G = C_m \times C_m$  is normal in  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ , and*

$$\text{Aut}_{\mathbb{K}}(\mathcal{X})/G \cong \begin{cases} C_2 \times C_2, & \text{if } a \neq 1; \\ D_4, & \text{if } a = 1. \end{cases}$$

*Proof.* Let  $\alpha \in \text{Aut}(\mathcal{X})$  be such that  $\alpha(\Omega_i) = \Omega_i$  for each  $i \in \{1, 2, 3, 4\}$ . Then  $\alpha(x) = c_1 x$  and  $\alpha(y) = c_2 y$ . It is then straightforward to see that  $c_1, c_2$  are  $m$ -th roots of the unity, whence  $\alpha \in G$ . This means that the kernel of the representation of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$  as permutation group on 4 letters is  $G$ , which is hence a normal subgroup of  $\text{Aut}_{\mathbb{K}}(\mathcal{X})$ . Also,  $|\text{Aut}_{\mathbb{K}}(\mathcal{X})| \leq 24m^2$ . We claim that there is no automorphism fixing one of the short orbits and acting as a 3-cycle on the other three. By contradiction, assume that such

an automorphism  $\alpha$  exists; without loss of generality, we may assume that  $\alpha(\Omega_3) = \Omega_3$ . Then either  $\alpha(\Omega_4) = \Omega_1$  or  $\alpha(\Omega_4) = \Omega_2$ , whence  $\alpha(x)$  either belongs to the Riemann-Roch space  $\mathcal{L}(R_1 + \dots + R_m)$  or  $\mathcal{L}(S_1 + \dots + S_m)$ . Then  $\alpha(x) = a_1 + \frac{b_1}{y}$  or  $a_2 + b_2 y$  by Lemma 6.15. Via straightforward computations, one can see that neither of the latter function can have zeroes in  $\Omega_3$ . The discussion at the beginning of the section finishes the proof.  $\square$

**Remark 6.18.** *The results of subsections 6.1 and 6.2 imply that  $\text{Aut}_{\mathbb{K}}(\mathcal{X}) = \text{Aut}_{\mathbb{F}_{q^2}}(\mathcal{X})$ .*

**Remark 6.19.** *We saw in Remark 5.10 that the curves  $X^n Y^2 + X^n + Y^2 = 1$  and  $\bar{X}^{2n} + \bar{Y}^2 = 1$  are birationally equivalent. It is not difficult to show that this is the only case of overlap between curves of type (I) and (II), listed at the beginning of this section.*

## Acknowledgments

The first author was supported by FAPESP-Brazil, grant 2013/00564-1. The second author was partially supported by GNSAGA - Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni of Italian INdAM. The authors would also like to thank Gábor Korchmáros and Massimo Giulietti for many useful conversations on the topic of this article.

## References

- [1] N. Arakelian and G. Korchmáros, *A characterization of the Artin-Mumford curve*, J. Number Theory **154** (2015), 278–291.
- [2] S. Fanali and M. Giulietti, *On the number of rational points of generalized Fermat curves over finite fields*, International Journal of Number Theory Vol. 8, No. 4 (2012) 1087–1097.
- [3] R. A. Hidalgo, A. Kontogeorgis, M. Leyton-Álvarez and P. Paramantzoglou, *Automorphisms of generalized Fermat curves*, preprint (2014) arXiv:1409.3063v2.
- [4] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, 2008.
- [5] A. Kontogeorgis, *The group of automorphisms of cyclic extensions of rational function fields*, J. Algebra **216** (1999), 665–706.
- [6] A. Kontogeorgis, *The group of automorphisms of the function field of the curve  $X^n + Y^m + 1 = 0$* , J. Number Theory **72** (1998), 110–136.
- [7] D. J. Madden, R. C. Valentini, *The group of automorphisms of algebraic function fields*, J. Reine Angew. Math. **343** (1983), 162–168.

- [8] H. G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994) 185–188.
- [9] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin and Heidelberg, 1993, vii+260 pp.
- [10] R. Valentini and M. Madan, *A Hauptsatz of L.E. Dickson and Artin-Schreier extensions*, J. Reine Angew. Math. **318** (1980), 156–177.